PLANEACIÓN Y EJECUCIÓN DE LA AUDITORIA INTERNA DEL SGSI DE PASSWORD CONSULTING SERVICES BAJO LA NORMA NTC-ISO/IEC 27001:2013 Y PLAN DE ACCIÓN DE LAS NO CONFORMIDADES ENCONTRADAS

ANDREA VIVEROS QUISOBONI

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2017

PLANEACIÓN Y EJECUCIÓN DE LA AUDITORIA INTERNA DEL SGSI DE PASSWORD CONSULTING SERVICES BAJO LA NORMA NTC-ISO/IEC 27001:2013 Y PLAN DE ACCIÓN DE LAS NO CONFORMIDADES ENCONTRADAS

ANDREA VIVEROS QUISOBONI

Trabajo de grado para optar al título de Especialista en Seguridad Informática

Director
ING. RICARDO HERRERA HERNÁNDEZ

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2017

Nota de aceptación

_____
_____
_____
_____
_____
_____
_____
_____

_____
Presidente del jurado

_____
Jurado

_____
Jurado

Bogotá, Diciembre de 2016

DEDICATORIA

Deseo dedicarles este trabajo de grado a Santiago Muñoz y Nicolás Muñoz. Es grato saber la fuerza y determinación que se posee cuando se quiere alcanzar algo.

AGRADECIMIENTOS

Agradezco a Dios por haberme dado los recursos necesarios para la realización del presente proyecto de grado que me permitirá obtener el título de Especialista en Seguridad Informática; también al ingeniero Ricardo Herrera quien fue el director del presente trabajo de grado por brindarme además de sus conocimientos como ingeniero su experiencia de vida y por brindar un acompañamiento continuo en este proceso; y al ingeniero Álvaro Escobar, Director de la Especialización.

CONTENIDO

Pág.

LISTA DE CUADROS

Pág.

LISTA DE FIGURAS

Pág.

INTRODUCCIÓN

Password Consulting Services S.A.S., es una empresa Colombiana, con orígenes en la universidad del Cauca, que ofrece servicios de consultoría en seguridad de la información tales como: seguridad de las tecnologías de información, consultoría en SGSI basados en la Norma NTC-ISO/IEC 27001:2013, servicios de consultoría en cumplimiento de Gobierno en Línea -GEL y servicios de outsourcing de seguridad, con más de 10 años de experiencia en empresas del sector privado y público.

Actualmente, Password cuenta con dos sedes, la casa matriz ubicada en la ciudad de Cali, Valle y la sede de Bogotá. Cuenta con más de 30 colaboradores directos y más de 20 consultores contratistas.

Password, se encuentra certificada en calidad con la norma NTC-ISO-IEC 9001:2015 y en seguridad de la información con la norma NTC-ISO-IEC 27001:2013, certificaciones que le han permitido posesionarse en el mercado de la seguridad de la información, razón por la cual para Password, el mantenimiento y re-certificación de su Sistema de Gestión de Seguridad de la Información – SGSI, es de gran importancia.

El presente informe plantea la estrategia adoptada para la planeación y ejecución de una auditoria interna del SGSI de Password Consulting Services, bajo la norma NTC-ISO-IEC 27001:2013, auditoría que le permitirá a la empresa mantener la certificación para el año 2016.

1 DEFINICIÓN DEL PROBLEMA

Password Consulting Services SAS (en adelante Password), es una empresa dedicada a la prestación de consultoría y asesoría en seguridad de la información. Su principal motivación por ser empresa de este sector de la seguridad, radica en el entendimiento de la importancia de la seguridad de la información y la necesidad de comunicarla a las empresas públicas y privadas, además de acompañarlas en el proceso de implementación de su SGSI. Razón por la cual actualmente Password tiene implementado y certificado un SGSI bajo la Norma NTC-ISO-IEC 27001:2013

Password, se ha encargado de fortalecer las competencias del recurso humano en diferentes áreas de la seguridad de la información; a través de cursos, diplomados, entrenamientos para profesionales en tecnología, charlas para gerentes y cursos para usuarios no técnicos. Los temas han sido enfocados hacia auditorías en ISO/IEC 27001:2013, análisis de riesgos, desarrollo de software seguro, seguridad en redes, entre otros.

Actualmente, la empresa no cuenta con un área de control interno, razón por la cual, las auditorías internas son gestionadas por los consultores de Password, que cuentan con certificaciones como auditores líderes e internos en ISO/IEC 9001:2015 y ISO/IEC 27001:2013. Sin embargo, las auditorías internas han sido realizadas por consultores de la sede de Cali, impidiendo una objetividad e imparcialidad total en los resultados. Adicionalmente, no se cuenta con los recursos económicos para contratar auditorías internas por terceros.

Teniendo en cuenta que para desarrollar auditorías internas es necesario contar con el recurso humano idóneo y multidisciplinario que apoye a toda la organización para poder atender auditorías externas, Password considera la opción de que la auditoria interna del segundo ciclo del 2016, sea realizada por un consultor de la sede Bogotá, con el fin de lograr objetividad e imparcialidad en los resultados. La pregunta es ¿La

gestión de una auditoría interna con personal de Password de la sede de Bogotá permite obtener resultados objetivos, con una baja inversión y con personal capacitado?

2 JUSTIFICACIÓN

El presente trabajo de grado se enfoca en la planeación y ejecución de la auditoría interna del SGSI, para el cumplimiento del programa anual de auditorías. Dado que para Password, es de vital importancia no solo validar el cumplimiento de las políticas y controles, así como también los requerimientos legales y la vigencia de las certificaciones internacionales.

Sin embargo, en el segundo semestre del 2016 los ingresos de la compañía no permiten la contratación de una auditoria interna contratada. Adicionalmente, existe falta de personal con las competencias como auditores internos y líderes en ISO 27001, en la sede de Cali para la ejecución de la auditoría interna del segundo ciclo del 2016, finalmente y dada la experiencia con los resultados en auditorías internas pasadas se requiere una auditoría imparcial para la ejecución de la auditoría interna en la sede Cali.

Por lo anterior la empresa decide realizar esta auditoría interna con personal de Bogotá con el fin de obtener un resultado más objetivo, económico y con personal capacitado.

Para la compañía esta auditoria permite conocer el estado real de su SGSI, que a su vez permite tomar medidas correctivas que lleven al cumplimiento y calidad de los sistemas existentes, adicionalmente se pretende que la auditoría contemple la totalidad de los requisitos y controles de la norma y retroalimente al personal auditado enfatizando en el ciclo de mejora continua de los procesos.

3 OBJETIVOS

3.1 OBJETIVO GENERAL.

Gestionar la auditoria interna del SGSI bajo la Norma NTC-ISO/IEC 27001:2013. En Password.

3.2 OBJETIVOS ESPECÍFICOS

3.2.1 Evaluar y estudiar el programa de auditoria anual de Password.

3.2.2 Identificar, valorar y definir los criterios de la auditoria del SGSI de Password.

3.2.3 Elaborar, ajustar y aprobar las listas de verificación para los diferentes procesos de la empresa incluidos en el alcance del SGSI.

3.2.4 Elaborar, ajustar y obtener aprobación del programa de auditoria para el SGSI de Password.

3.2.5 Ejecutar la auditoria en los diferentes procesos de acuerdo al programa de auditoria y con las listas de verificación aprobadas.

3.2.6 Elaborar y presentar el informe final de la auditoria registrando los hallazgos encontrados durante la actividad.

3.2.7 Elaborar y presentar un plan de cierre de no conformidades encontradas en la auditoria.

4 MARCO REFERENCIAL

4.1 MARCO CONCEPTUAL

4.1.1 Auditoria. La palabra auditoria viene del latín *auditorius* y de esta proviene “auditor”, el que tiene la virtud de oír; el diccionario lo define como “revisor de cuentas colegiado”.

El auditor tiene la virtud de oír y revisar cuentas, pero debe estar encaminado a un objetivo específico, que es el de evaluar la eficiencia y eficacia con la se opera un sistema, con el objetivo de identificar oportunidades de mejora, tomar decisiones y corregir errores en los procesos y procedimientos.

Actualmente las normas y procedimientos para la gestión de auditorías en Sistemas de Gestión de Seguridad de la Información hacen parte de una profesión. Estas pueden estar basadas en las experiencias de otras profesiones, con algunas características propias y siempre guiándose por el concepto de que la auditoria y además de permitir mejorar lo existente, corregir errores y proponer alternativas de solución[1].

4.1.2 Construcción de una auditoria interna eficaz. El objetivo del departamento de auditoría interna debe ser promover los controles internos y ayudar a la empresa a desarrollar soluciones efectivas teniendo en cuenta el costo/beneficio para brindar solución a los problemas evidenciados. Este departamento agrega valor a la empresa, a través de su experiencia y conocimiento de los controles internos y su forma de evaluarlos. De esto se pude concluir que la misión consta de dos puntos:

[1] ECHENIQUE GARCIA, José Antonio. Auditoria Informática. 2 ed. México, México.: McGraw-Hill, 2001. p. 2-3.

4.1.2.1 Garantizar independencia de la auditoría, debido a que conocen los controles internos de la empresa y pueden hacer que funcionen eficazmente.

4.1.2.2 Mejorar continuamente los controles internos de la empresa, se deben identificar las debilidades del control y desarrollar soluciones costo/efectividad para abordar esas diferencias[2].

4.1.3 La independencia. El gran mito, según Webster´s College Dictionary universal, a independencia es “La calidad del estado de ser independiente” – “No influenciados o controlados por otros”. Pero esto no es cierto, debido a que se deben reportar informes al presidente de la organización y al CEO, ya que el CEO es quien controla el presupuesto para el departamento de auditoría. Las personas que realizan la auditoria deben realizar su trabajo objetivamente y no subjetivamente3.

4.1.4 Equipo auditor. La importancia del grupo de auditoría y su departamento, se debe a que se pueden identificar correcciones a los problemas a tiempo, beneficiando en costo (disminuyendo costos) y a su vez se podrán agregar controles después de identificar los casos. El departamento de auditoría también puede proporcionar una evaluación de los controles propuestos y aplicados4.

4.1.5 Métodos de consultoría y participación temprana. Estos métodos se proponen para promover los controles internos en la organización, fuera de las auditorias formales y son los siguientes:

4.1.5.1 Participación temprana: El cambio cuesta más que la primera implementación.

---

[2] DAVIS, Chris y Schiller, Mike y Wheeler Kevin. IT Auditing: Using Controls to Protect Information Assets. 2 ed. Estados Unidos.: McGraw-Hill, 2011. p. 3

[3] Ibíd., p.5

[4] Ibíd., p.6

4.1.5.2 Auditoria informal: No documentar.

4.1.5.3 Compartir conocimientos: A través de sitio web e email.

4.1.5.4 Directriz de control: El control no debe ser una política, pero si debe estar direccionado a cumplir con las políticas de la organización.

4.1.6 Problemas comunes, mejores prácticas y soluciones innovadoras. Muy pocas veces se comparan las auditorías realizadas entre organizaciones del mismo sector y se ignora la gran utilidad que pueden llegar a traer para las organizaciones la revisión de esas auditorías, cuando se realiza una auditoria y se encuentran hallazgos comunes es importante publicarlos en el sitio web del departamento del auditoria y enviar e-mail a todo el personal pertinente informando el hallazgo y los controles a aplicar[5].

4.1.7 Herramientas. Se pueden compartir las herramientas con otros grupos para permitir auto-evaluación de los controles. Sin embargo, es importante establecer políticas, permisos, horas y zonas de aplicación de estas herramientas, pero no se recomienda compartir herramientas que comprometan información sensible, personal o que viole la integridad6.

4.1.8 El papel del equipo de auditoria. Existen auditores dedicados a: (aplicaciones, extracción y análisis de datos y auditoria de TI). Para ser auditor de cada uno de estos campos no es necesario ser especialista, pero si certificado en (CISA-CISSP) y tener experiencia en la realización de controles generales.

---

[5] DAVIS, op. cit, p. 9

[6] Ibíd., p.16

4.1.9 Mantenimiento de la experiencia. Invertir en renovar la capacitación y el conjunto de habilidades, esta renovación constante se debe realizar periódicamente debido a que la tecnología varía constantemente.

Con todo este proceso lo que se busca es que el aporte que brinde el departamento de TI, no solo sea de mantenimiento de software como la gran parte de personas de la organización lo piensa, el grupo de auditoría de TI, debe aliarse al grupo de auditoría externa y brindar juntos un valor agregado a la organización donde se permita contar con los controles pertinentes para para cada proceso de la organización[7].

4.1.10 Proceso de auditoría. Controles internos: El concepto de control interno es clave en la auditoría. Los controles internos, son mecanismos que garantizan el correcto funcionamiento de los procesos dentro de la empresa.

4.1.11 Los controles Internos. Se pueden clasificar en preventivo, detectivo y reactivo, pueden tener implementaciones administrativas, técnicas o físicas. Las implementaciones administrativas incluyen elementos tales como políticas y procesos.

4.1.11.1 Controles preventivos. Los controles preventivos están diseñados para evitar que un evento negativo suceda. Desde el punto de vista teórico estos son los controles que deben privilegiarse.

4.1.11.2 Controles detectivos. Están diseñados para grabar los eventos negativos que hayan ocurrido.

[7] DAVIS, op. cit, p. 21

4.1.11.3 Controles de reactivos (correctivos). Estos controles se ubican entre los controles preventivos y los detectivos y se destacan por detectar de manera sistemática cuando los malos sucesos han ocurrido y corregir la situación[8].

4.1.12 Determinar qué auditar. El plan de auditoría debe focalizarse en las áreas con mayor riesgo y en donde se pueda agregar mayor valor. Debe ser eficiente y eficaz el uso de los recursos limitados por el gasto. La auditoría del SGSI debe ser un proceso metódico y lógico que garantice transparencia y calidad.[9]

Es importante estudiar y validar los criterios de auditoria, para esto se requiere solicitar información del SGSI de la empresa como: política, alcance, objetivos, manuales y procedimientos del SGSI. Se debe tener en cuenta los requerimientos de la Norma NTC-ISO-IEC 27001:2013.

4.1.13 Metodología de la auditoria. A continuación, se describen los pasos de la metodología para el desarrollo de auditoria

4.1.13.1 Planificación. Antes de empezar cualquier trabajo de auditoría, se debe organizar un plan de auditoria. Si el proceso de planificación es ejecutado eficazmente, llevara al equipo de auditoría al éxito[10].

4.1.13.2 El trabajo de campo y documentación. Este paso es el grueso de la auditoría, permite al equipo auditor evidenciar la gestión del SGSI, a través de entrevistas, revisiones y validación de datos. Para posteriormente, analizados y obtener posibles riesgos, No conformidades, observaciones y oportunidades de mejora[11].

---

[8] DAVIS, op. cit, p. 35 y 36

[9] DAVIS, op. cit, p. 38

[10] DAVIS, op. cit, p. 43

[11] DAVIS, op. cit, p. 46

4.1.13.3 Descubrimiento de Problemas y validación. Mientras se ejecuta el trabajo de campo, los auditores elaborarán una lista de problemas potenciales y generarán la validación de los mismos en el campo[12].

4.1.13.4 Desarrollo de soluciones. Después de haber identificado los problemas potenciales en las áreas auditadas y una vez validado los hechos y riesgos se puede trabajar en desarrollar el plan de acción o cierre de no conformidades[13].

4.1.13.5 Emisión de informe. Posteriormente se debe redactar el Informe de auditoría. El informe de auditoría es el medio por el cual se documentan los resultados de la auditoría. Este informe permite llevar un registro de la auditoría, resultados y planes de acción[14].

4.1.13.6 Seguimiento del problema. Es común para los auditores sentir que la auditoría está "Terminada" una vez que el informe de auditoría se ha expedido. Sin embargo, la emisión de un informe de auditoría no añade valor a la empresa, a menos que se vean los resultados de las medidas adoptadas[15].

4.2 MARCO LEGAL

La Organización Internacional de Normalización, popularmente conocida como ISO/IEC, es la organización que se ocupa de establecer las normas de fabricación, de comunicación y de comercialización, tanto de productos como de servicios, en el plano internacional. Lo que básicamente propone la ISO/IEC, es estandarizar las normas de seguridad. En atención al proyecto de grado es necesario tener en cuenta las normas técnicas colombianas que a continuación se describen.

---

[12] DAVIS, op. cit, p. 47

[13] DAVIS, op. cit, p. 48

[14] DAVIS, op. cit, p. 52 y 53

[15] DAVIS, op. cit, p. 58

4.2.1 Norma NTC-ISO/IEC 19011:2011. Desde la primera publicación de esta norma internacional en el 2002, se han publicado un gran número de normas para el sistema de gestión. Por esta razón, el comité ISO, considera la necesidad de tener un alcance más amplio para la auditoria de sistemas de gestión, así como proveer lineamientos más generales. Esta norma internacional proporciona directrices para la gestión de auditorías a sistemas de gestión, incluyendo los principios de auditoría, el manejo de un programa de auditoría y la realización de las auditorías a sistemas de gestión, así como directrices sobre la evaluación de competencia de los individuos involucrados en el proceso de auditoría, incluyendo el personal que maneja el programa de auditoría, los auditores y los equipos de auditoría[16]. Esta norma es aplicable a todas las organizaciones que requieran llevar a cabo auditorías internas o externas a sistemas de gestión o manejar un programa de auditoría.

4.2.2 Norma ISO/IEC 27000. Publicada el 1 de mayo de 2009, revisada con una segunda edición de 01 de diciembre de 2012, una tercera edición del 14 de enero de 2014 y una última edición en febrero de 2016. Esta norma proporciona una visión general de las normas que componen la serie 27000, indicando para cada una de ellas su alcance de actuación y el propósito de su publicación. Recoge todas las definiciones para la serie de normas 27000 y aporta las bases de la importancia de la implantación de un SGSI, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción de los pasos para el establecimiento, monitorización, mantenimiento y mejora de un SGSI (la última

[16] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS. Directrices para la auditoria de sistemas de gestión. Bogotá D.C.: ICONTEC, 2011. NTC-ISO/IEC 19011.

edición no aborda el ciclo Plan-Do-Check-Act para evitar convertirlo en el único marco de referencia para la mejora continua)[17].

4.2.3 Norma NTC-ISO/IEC 27001. La última versión de la norma NTC-ISO/2700 es la 2013. Esta norma ha sido elaborada para suministrar registros para el establecimiento, implementación, mantenimiento y mejora continua de un SGSI. La adopción de un SGSI es una decisión estratégica para una organización. El establecimiento de este sistema de gestión debe estar orientado a los objetivos y necesidades de la organización, los requisitos de seguridad, los procesos organizacionales empleados, el tamaño y estructura de la organización[18].

Uno de los objetivos del SGSI es preservar la confidencialidad, la integridad y la disponibilidad de la información, a través de la gestión de riesgo. Esta norma es certificable.

4.2.4 Norma ISO/IEC 27002. Publicada desde el 1 de julio de 2007, es el nuevo nombre de ISO 17799:2005, Esta Norma Internacional está diseñada para uso por parte de las organizaciones, como referencia para la selección de controles dentro del proceso de implementación de un SGSI (SGSI) con base en la ISO/IEC 27001:2013, o como un documento guía para organizaciones que implementan controles de seguridad de la información comúnmente aceptados. Esta Norma es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO

[17] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI). Visión general y Vocabulario. Bogotá D.C.: ICONTEC, 2016. NTC-ISO/IEC 27000

[18] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI). Requisitos. Bogotá D.C.: ICONTEC, 2013. NTC-ISO/IEC 27001

27001 contiene un anexo que resume los controles de ISO 27002:2005. Actualmente, la última edición de 2013 este estándar ha sido actualizada a un total de 14 Dominios, 35 Objetivos de Control y 114 Controles[19].

4.2.5 Norma ISO/IEC 27003. La más reciente versión fue publicada el 12 de diciembre del 2012. No certificable. Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001:2013. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI. Tiene su origen en el anexo B de la norma BS 7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación[20].

4.2.6 Norma NTC-ISO/IEC 27005. La más reciente versión fue publicada en agosto del 2009, esta norma suministra directrices para la gestión en la seguridad de la información, además brinda soporte a los conceptos generales que se especifican en la norma NTC-ISO/IEC 27001 y está diseñada para facilitar la implementación satisfactoria de la seguridad de la información con base en el enfoque de la gestión del riesgo[21].

---

[19] INSTITUTO COLOMBIANO DE NORMAS TECNICAS. Tecnología de la información. Técnicas de seguridad. Código de Práctica para controles de seguridad de la información. Bogotá D.C.: ICONTEC, 2015. GTC-ISO/IEC 27002

[20] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS. Tecnología de la información. Técnicas de seguridad. Guía de implementación de un sistemas de gestión de seguridad de la información. Bogotá D.C.: ICONTEC, 2012. GTC-ISO/IEC 27003

[21] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS. Tecnología de la información. Técnicas de seguridad. Gestión del riesgo en seguridad de la información. Bogotá D.C.: ICONTEC, 2009. NTC-ISO/IEC 27005

5 DISEÑO METODOLÓGICO

El tipo de investigación es aplicada correlacional, debido a que permite medir y establecer el grado de relación entre las variables (SGSI y PC).

5.1 HIPÓTESIS

Hipótesis Investigativa: Con la auditoria interna al SGSI se garantiza seguimiento y cumplimiento de las políticas, controles y procedimientos del SGSI de Password.

.

Hipótesis Nula: Con la auditoria interna al SGSI no se garantiza seguimiento y cumplimiento de las políticas, controles y procedimientos del SGSI de Password.

5.2 VARIABLES

En el cuadro 1. Variables, se detallan las variables escogidas y su descripción.

Cuadro 1. Variables

Variable	Abreviación	Descripción	Tipo
Independiente	SGSI	Auditoria del SGSI	Cualitativa
Dependiente	PC	Implementación de las políticas y controles	Cuantitativa - continuas

Fuente: Autor

6 PHVA DE EJECUCIÓN DE LA AUDITORÍA

La ejecución del trabajo de grado se realizó de acuerdo a la metodología propuesta por la norma NTC – ISO/IEC 19011:2011, directrices para la auditoría de sistemas de gestión.

La auditoría se realizó de acuerdo a la metodología del ciclo PHVA. Tal y como lo muestra la figura 1.

Figura 1. Ciclo PHVA

Fuente: Autor

6.1 FASE 1: PLANEACIÓN DE LA AUDITORÍA

A continuación se relacionan las actividades requeridas para la planeación de la auditoria interna a Password.

6.1.1 Actividad 1. Se elaboró el Plan de Trabajo, cronograma, riesgos, procedimientos y se gestionaron los recursos necesarios para la auditoría de primera parte al SGSI de Password.

6.1.2 Actividad 2. Se realizó una reunión con la funcionaria de Password, encargado del Sistema Integrado de Gestión y se definió el alcance de la auditoria.

6.1.3 Actividad 3. Se planeó la auditoría interna y se estudió la documentación e información de las áreas del alcance de la auditoría interna en Password.

6.1.4 Actividad 4. Se elaboró el plan de auditoría teniendo en cuenta los siguientes aspectos:

6.1.4.1 Alcance de la auditoria. (Proceso de gestión de proyectos, gestión estratégica, gestión de tecnología, gestión comercial, gestión de calidad y gestión de recursos humanos), Procesos del alcance de la certificación actual en la norma NTC-ISO/IEC 27001:2013.

- Procedimientos del programa de auditoría.
- Criterios de auditoría.
- Métodos de auditoría.
- Selección de equipos auditores.
- Recursos necesarios, incluyendo viajes y hospedaje.

- Procesos para manejo de confidencialidad, seguridad de la información, salud y seguridad y otros temas similares.

6.1.5 Actividad 5. Seleccionar la metodología que se va a utilizar para la ejecución de las auditorías, (entrevista en sitio de trabajo).

6.1.6 Actividad 6. Seleccionar y asignar las responsabilidades de la auditoría individual al líder del equipo auditor.

6.1.7 Actividad 7. Elaboración de las listas de verificación para cada uno de los procesos que hacen parte del alcance definido previamente.

6.1.8 Actividad 8. Enviar las listas de verificación para la auditoría a Password, para la respectiva aprobación por parte de la gestora de calidad.

6.1.9 Actividad 9. Aprobación de las listas de verificación en el formato enviado previamente por Password, teniendo en cuenta los criterios definidos previamente.

6.1.10 Actividad 10. Programación de la visita para ejecución de la auditoría interna al SGSI de Password.

6.2 FASE 2: EJECUCIÓN DE LA AUDITORÍA

6.2.1 Actividad 11. Reunión de apertura de la auditoría interna con los líderes de las áreas que son parte del alcance de la auditoría Password.

6.2.2 Actividad 12. Diligenciar un acta de inicio de la auditoría donde se establezcan las condiciones, es decir, objetivo, alcance, equipo auditor, el programa de auditoria y se definan los cambios solicitados al programa de auditoria.

6.2.3 Actividad 13. Ejecución de los planes de auditoría a los procesos definidos en el alcance de acuerdo a las listas de verificación previamente definidas.

6.3 FASE 3 ELABORACIÓN DE INFORMES

6.3.1 Actividad 14. Recolección y Verificación de la información relevante a los objetivos, alcance y criterios de la auditoría y evidencias que conduzcan a encontrar hallazgos de auditoría.

6.3.2 Actividad 15. Evaluar los hallazgos contra los criterios de la auditoría a fin de determinar la veracidad de estos.

6.3.3 Actividad 16. Elaborar el informe preliminar de auditoria, especificando observaciones, no conformidades menores y mayores.

6.3.4 Actividad 17. Realizar reunión de cierre de auditoría con los líderes de los procesos, en esta reunión se debe presentar el informe preliminar de la auditoria.

6.3.5 Actividad 18. Elaborar acta de cierre de auditoria, dejar evidencia de las actividades de la reunión.

6.4 FASE 4. MONITOREO DE AUDITORÍA

6.4.1 Actividad 20. Validar si se cumplieron los objetivos de la auditoria.

6.4.2 Actividad 21. Evaluar la auditoría, solicitar evaluación de auditores

6.5 RESULTADOS DE LA AUDITORÍA

Se elaboró el plan de auditoria el cual incluye:

.

6.5.1 Alcance de la auditoría. Se define como alcance de la auditoria interna del SGSI de Password, los siguientes procesos:

- Gestión de proyectos.
- Gestión estratégica.
- Gestión de tecnología.
- Gestión comercial.
- Gestión de Integral.
- Gestión de recursos humanos.

Posteriormente se realizó una reunión con la líder del Sistema Integrado de Gestión de Password, con el fin de socializar el plan de auditoria

6.5.2 Criterios de auditoría. Una vez aprobado el alcance y obtenida la información se definieron los criterios por proceso así:

6.5.2.1 Gestión integra. Se establece como criterios: la norma NTC-ISO/IEC 27001:2013, la caracterización del proceso vigente, los procedimientos de auditorías internas, de acciones correctivas y preventivas, de gestión de incidentes, gestión de vulnerabilidades, gestión de activos, clasificación y etiquetado, gestión de cambios vigentes y la metodológica gestión de riesgos.

6.5.2.2 Gestión comercial. Se establece como criterios: la caracterización del proceso, los documentos del proceso, las políticas de seguridad de la información y los requisitos de la norma NTC-ISO/IEC 27001:2013.

6.5.2.3 Gestión estratégica. Se establece como criterios; la norma NTC-ISO/IEC 27001:2013, el manual del SIG vigente, la matriz de comunicaciones y la caracterización del proceso.

6.5.2.4 Gestión de talento humano. Se establece como criterios; la norma NTC-ISO/IEC 27001:2013, el procedimiento de gestión de talento humano, el procedimiento de contratistas, el manual del SIG y la caracterización del proceso.

6.5.2.5 Gestión de proyectos: Se establece como criterios; la norma NTC-ISO 27001:2013, el manual del SIG vigente, la caracterización del proceso de proyectos, el procedimiento análisis de seguridad, el procedimiento análisis forense, el procedimiento control de servicio no conforme y el procedimiento consultoría.

6.5.2.6 Gestión tecnológica: Se establece como criterios; La norma ISO 27001:2013, la caracterización del proceso, los procedimientos aplicables, el manual de políticas de seguridad, procedimientos de tecnología y la declaración de aplicabilidad.

6.6 METODOLOGÍA DE LA AUDITORÍA

Se define como metodología para la ejecución de la auditoria, entrevistas en el puesto de trabajo de cada uno de los auditados

6.7 EQUIPO AUDITOR

El equipo auditor es conformado por la ingeniera Andrea Viveros Quisoboni, Coordinador de Proyectos Bogotá y por la señora Diana Castillo, líder de calidad de Password Consulting Services.

6.8 RECURSOS

Dado que el alcance de la auditoría interna, es en la ciudad de Cali Valle, se definen como recursos para la auditoría, los días laborales, los viáticos de los 3 días en la ciudad de Cali y los tiquetes de avión.

6.9 ACUERDO DE CONFIDENCIALIDAD

Previo a la fecha de la auditoría se verifica la firma del acuerdo de confidencialidad contractual de la ingeniera Andrea Viveros y la señora Diana Castillo.

6.10 PLAN DE AUDITORÍA

Posteriormente se procedió a elaborar y enviar el plan de auditoría a Password, sede Cali de acuerdo el alcance, los criterios, el equipo auditor y los auditados. Previa aprobación por parte de la alta dirección de la empresa se ejecutó la actividad que fue programada y ejecutada para el 20, 21 y 22 de septiembre de 2016.

6.11 LISTAS DE VERIFICACIÓN O LISTAS DE CHEQUEO

Se elaboraron los planes de auditoría teniendo en cuenta los criterios anteriormente definidos los cuales se presentan en el siguiente cuadro, ver cuadro 2, de requisitos aplicables de la norma NTC-ISO/IEC 27001:2013.

Cuadro 2.Matriz de requisitos aplicables de la norma NTC-ISO/IEC 27001:2013.

Matriz requisitos aplicables (NORMA ISO 27001:2013 VS. PROCESOS)			
No.	Proceso	Requisitos	Controles anexo A.
1	Gestión comercial	6.1.2,6.1.3,8.2, 8.3,10.1	A.6.1.2,A.8.2.2,A.8.2.3,A.11.2.8,A.11.2.9,A.16.1.2, A.16.1.3,A.18.1.3, A.18.1.4, A.18.2.2
2	Gestión de proyectos	6.1.2,6.1.3,8.2, 8.3,10.1	A.6.1.2,A.6.1.5,A.8.2.2,A.8.2.3,A.11.2.8,A.11.2.9,A. 16.1.2, A.16.1.3A.18.1.3, A.18.1.4, A.18.2.2
3	Gestión estratégica	6.1.2,6.1.3,7.1,8.1, 8.2, 8.3,10.1	A.6.1.2,A.8.2.2 A.8.2.3,A.11.1,A.11.2.8,A.11.2.9, A.15,A.16.1.2, A.16.1.3,A.18.1.3, A.18.1.4, A.18.2.2
4	Gestión talento humano	5.3,6.1.2,6.1.3,7.2, 7.3,8.2, 8.3,10.1	A.6.1.1, A.7,A.8.1.4,A.8.2.2 A.8.2.3,A.11.2.8,A.11.2.9,A.16.1.2, A.16.1.3,A.18.1.3, A.18.1.4, A.18.2.2
5	Gestión de tecnología	6.1.2,6.1.3,8.2, 8.3,10.1	A.6.1.2, A.6.2,A.8.1.3,A.8.1.4,A.8.2.2,A.8.2.3,A.8.3.1, A.8.3.2, A.8.3.3,A.9.1, A.9.2, A.9.3, A.9.4, A.10, A.11.2, A.12.1.1,A.12.1.3,A.12.1.4,A.12.2,A.12.3, A.12.4,A.12.5,A.12.6.2, A.13, A.14.1,A.14.2.4,A.16.1.2, A.17.2,A.18.1.3, A.18.1.4, A.18.1.5,A.18.2.2,,A.18.2.3
6	Gestión integral	4.4,6.1,7.5,8.1,8.2, 8.3,9.1,9.2,10.1	A.6.1.2,A.6.1.3, A.6.1.4, A.8.1.1, A.8.1.2,A.8.1.3,A.8.2.1,A.8.2.2,A.8.2.3,A.11.2.8,A.1 1.2.9,A.12.1.2, A.12.6.1,A.12.7,A.13,A.16,A.17,A.18.1.3, A.18.1.4,A.18.2.1,A.18.2.2
	Fecha de actualización		18/09/2016

Fuente: Autor

6.12 EJECUCIÓN DE LA AUDITORÍA

Se ejecuta la auditoria de acuerdo al programa de auditoría previamente aprobado, se realiza la reunión de inicio, con una presentación en la cual se explican los objetivos, criterios, el equipo auditor, se pone a consideración el programa de auditoría en el caso de requerir un cambio en el itinerario.

Posteriormente se inicia con las entrevistas de acuerdo a la programación durante los dos días propuestos. Una vez ejecutadas las entrevistas en su totalidad se procede a entregar el primer informe la auditoría y se revisen las retroalimentaciones. La actividad queda consignada en el acta de cierre de auditoría.

6.13 ELABORACIÓN DE INFORMES

Finalmente se realiza la rrecolección y verificación de la información que fue relevante para los objetivos, el alcance, los criterios de la auditoría y las evidencias que llevaron a definir hallazgos de auditoría, se procedió a evaluar los hallazgos contra los criterios de la auditoría, se determinó la veracidad de los hallazgos. Se presenta el informe preliminar de auditoria en la reunión de cierre de auditoría en esta reunión se logró especificar observaciones y No conformidades menores. Posteriormente, se envía el informe definitivo de la auditoria interna del SGSI de Password. A continuación, se describen los hallazgos de manera gerencial.

6.14 NIVEL DE MADUREZ DEL SGSI DE PASSWORD

6.14.1 Definiciones del nivel de madurez. Para determinar el nivel de madurez se establece a grandes rasgos la eficacia del control validado durante las entrevistas, así como la capacidad de cobertura de los mismos dentro de la organización y sus actividades dando un porcentaje a cada control para finalmente promediar el cumplimiento total del objetivo de control. Para esto se han determinado seis niveles

de madurez distribuidos en diferentes rangos porcentuales. Los cuales se pueden evidenciar en el cuadro 3:

Cuadro 3. Cuadro Nivel de Madurez

Nivel de madurez	Límite inferior	Límite superior
Optimizado	91%	100%
Administrado	71%	90%
Definido	61%	70%
Repetible	41%	60%
Inicial	16%	40%
Inexistente	0%	15%

Fuente: Password Consulting Services.

A continuación, se definen cada uno de los niveles definidos en el cuadro 3:

Nivel 0 - Inexistente: Carencia completa de esta práctica o desarrollo de algunas actividades y/o procesos alrededor de la misma.

Nivel 1 - Inicial: Se reconoce la importancia de esta práctica por lo que se desarrollan y documentan algunas actividades y/o procesos alrededor de la misma.

Nivel 2 - Repetible: Se desarrollan actividades y/o procesos, sin embargo no han sido documentadas, ni hay entrenamiento ni comunicación formal de la misma. Se deja la responsabilidad al individuo.

Nivel 3 - Definido: Esta práctica se ha estandarizado, documentado y ha sido difundida.

Nivel 4 - Administrado: Esta práctica se monitorea y mide su cumplimiento. Se toman medidas cuando los procesos y/o actividades no están logrando su objetivo.

Nivel 5 - Optimizado: Los procesos se han redefinido al nivel de mejor práctica. Existe evidencia de la mejora continua.

6.14.2 Resultado del nivel de madurez del SGSI de Password. Producto de la auditoría realizada a Password, se determina que el nivel de madurez del SGSI, es del 88.5%. A continuación, se explican los resultados obtenidos tanto en las clausulas como en el anexo A, de la Norma NTC-ISO/IEC 27001:2013.

De acuerdo a los resultados detallados por cláusulas de la Norma NTC-ISO/IEC 27001:2013. Se define que el nivel de madurez de las cláusulas del SGSI en Password, es un nivel Administrado, es decir, que esta práctica se monitorea y se mide su cumplimiento. Se toman medidas cuando los procesos y/o actividades no están logrando su objetivo. En el cuadro 4 se listan los resultados obtenidos en cada una de las cláusulas de la Norma NTC-ISO/IEC 27001:2013.

Cuadro 4. Nivel de madurez cláusulas de la Norma NTC-ISO/IEC 27001:2013

Ítem	Cláusulas del SGSI	Cláusulas	Nivel de madurez cláusulas
4..	Contexto de la organización	**100%**	**Optimizado**
5..	Liderazgo	**88%**	**Administrado**
6..	Planificación	**95%**	**Optimizado**
7..	Soporte	**88%**	**Administrado**
8..	Operación	**67%**	**Definido**
9..	Evaluación del desempeño	**98%**	**Optimizado**
10..	Mejora	**91%**	**Optimizado**
Nivel de madurez		**90%**	**Administrado**

Fuente: Autor

De acuerdo a los resultados detallados por los dominios del anexo A de la Norma NTC-ISO/IEC 27001:2013. Se define que el nivel de madurez del SGSI en Password, es un nivel Administrado, es decir, que esta práctica se monitorea y se mide su cumplimiento. Se toman medidas cuando los procesos y/o actividades no están logrando su objetivo. En el cuadro 5 se listan los resultados obtenidos en cada una de los dominios de la Norma NTC-ISO/IEC 27001:2013.

Cuadro 5. Nivel de madurez de los dominios del anexo A de la Norma NTC-ISO/IEC 27001:2013.

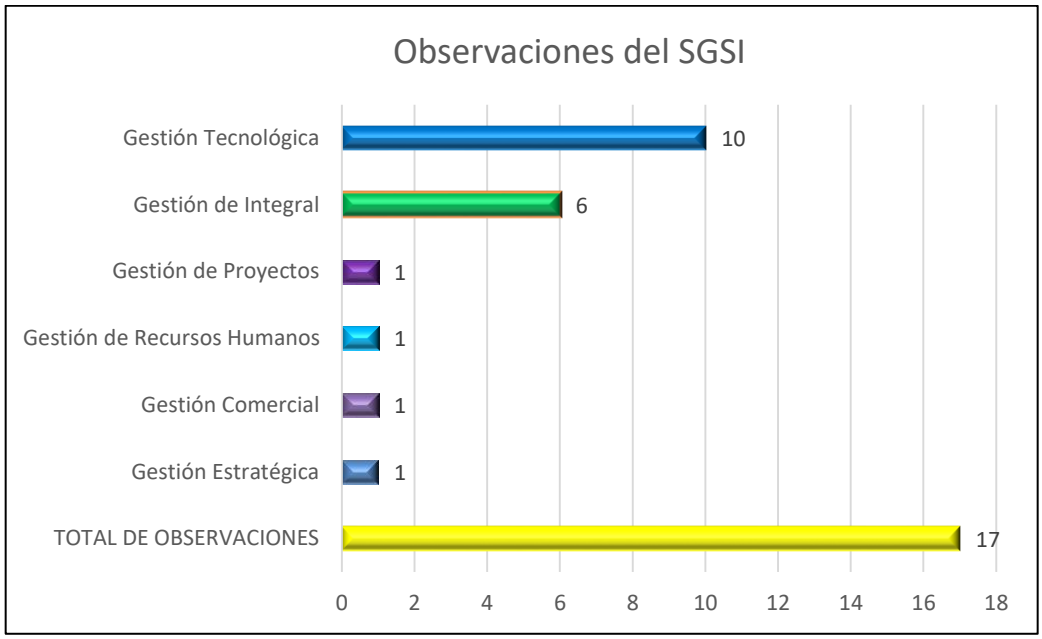
Ítem	Dominios	Controles	Nivel de madurez Dominios
A.5..	Política de Seguridad de la Información	100%	Optimizado
A.6..	Organización de la Seguridad de la Información	100%	Optimizado
A.7..	Seguridad en los Recursos Humanos	83%	Administrado
A.8..	Gestión de los activos	50%	Repetible
A.9..	Control de Acceso	96%	Optimizado
A.10..	Criptografía	50%	Repetible
A.11..	Seguridad Física y del Entorno	90%	Administrado
A.12..	Seguridad de las Operaciones	86%	Administrado
A.13..	Seguridad de las Comunicaciones	100%	Optimizado
A.14..	Adquisición, Desarrollo y Mantenimiento de Sistemas	100%	Optimizado
A.15..	Relaciones con los Proveedores	100%	Optimizado
A.16..	Gestión de incidentes de Seguridad de la Información	57%	Repetible
A.17..	Aspectos de seguridad de la información de la Gestión de Continuidad de Negocio	100%	Optimizado
A.18..	Cumplimiento	100%	Optimizado
NIVEL DE MADUREZ		**87%**	**Administrado**

Fuente: Autor

6.14.3 Aspectos por mejorar/observaciones de la auditoría. Como resultado de la auditoría se evidenciaron un total de 17, aspectos por mejorar y/o observaciones; El proceso de gestión tecnológica obtuvo un total de 10 observaciones correspondientes al 50%, el proceso de gestión integral obtuvo un total de 6 observaciones correspondientes al 30%, el proceso gestión de recursos humanos,

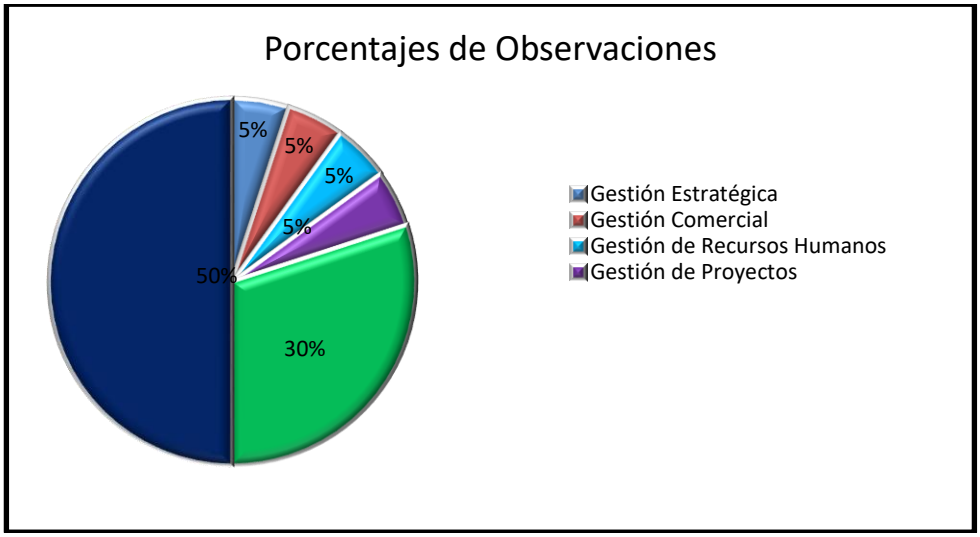
obtuvo una observación correspondiente al 5%, los procesos de gestión de proyectos, gestión comercial y gestión estratégica obtuvieron observaciones compartidas correspondientes al 15% restante, como se observa en las Figuras 2 y 3.

Figura 2. Observaciones del SGSI



Fuente: Autor

Figura 3. Porcentaje de observaciones



Fuente: Autor

En el cuadro 6, se pueden evidenciar las observaciones por proceso, el numeral de la norma con la que se relaciona y el control relacionado.

Cuadro 6. Observaciones detalladas

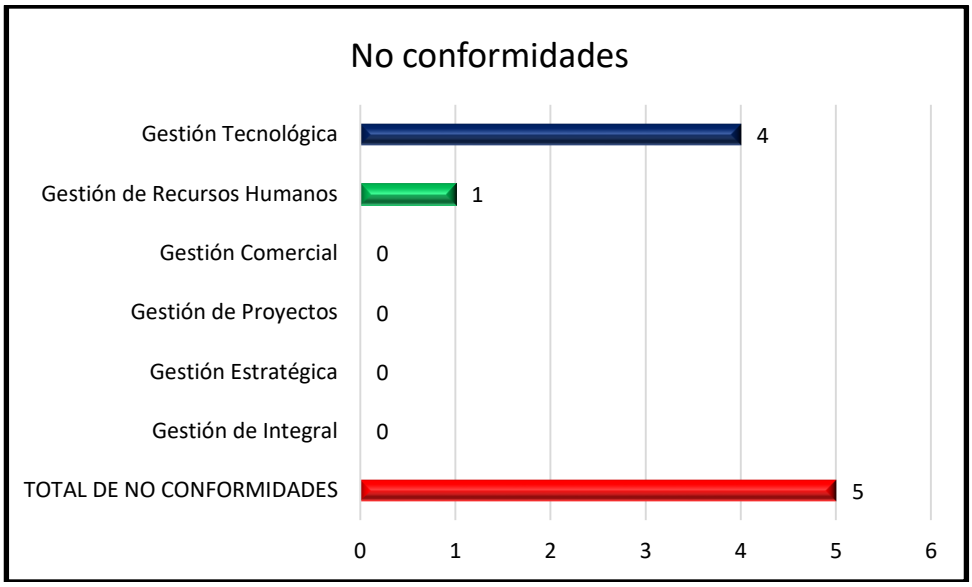
Proceso	Numeral ISO 27001	Control
Gestión integral y todos los procesos	A.8.2.1	Clasificación de Activos
	A.8.2.2	Etiquetado de Activos
	A.8.2.3	Manejo de Activos
	6.1.2	Valoración de Riesgos
	6.1.3	Tratamiento de Riesgos
	A. 7.2.2	Toma de Conciencia
	A.6.1.4	Contacto con Grupo de Interes Especial
	A.16.1.1	Responsabilidad de Incidentes
	7.2 Literal a)	Determinar competencias necesarias
Gestión Talento Humano	7.2	Inducción
	A.7.3.1	Cambio de responsabilidades-Oficial
Gestión de tecnología	A.8.1.1	Inventario de activos
	A.8.1.2	Propietario de activos
	A.8.1.3	Uso de aceptable de activos
	A.8.3.2	Dispocisión de los Medios
	A.9.3	Cumplimiento de Políticas con Contraseñas
	A.10	Criptografía-No adecuada gestión
	A.14.1.1	Definir requisitos de seguridad de los SI
	A.16.1.6 y A. 16.1.7	Aprendizaje y recolección de evidencias en Incidentes
	A.11.2.2	Suministro de Energia

Fuente: Autor

6.14.4 No conformidades. Como resultado de la auditoría se evidenciaron un total de 5 No conformidades menores; el proceso de gestión tecnológica obtuvo un total de 4. No conformidades menores correspondientes al 80%, el proceso de recursos humanos obtuvo una No conformidad correspondiente al 20%, como se evidencia en las figuras 4 y 5.

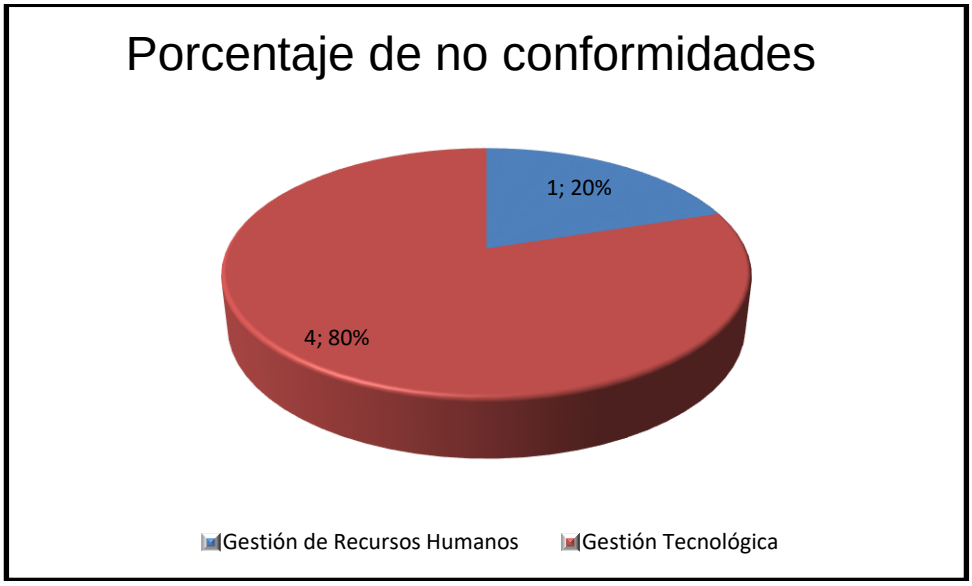
Los procesos de gestión estratégica, gestión integral, gestión de proyectos y gestión comercial no obtuvieron No conformidades.

Figura 4. No conformidades



Fuente: Autor

Figura 5. Porcentaje de no conformidades



Fuente: Autor

En el cuadro 7, se pueden evidenciar las No conformidades identificadas, el proceso al que pertenecen, el numeral de la norma con la que se relaciona y el control relacionado.

Cuadro 7. No conformidades

Proceso	Numeral ISO/IEC 27001:2013	Control
Gestión talento humano	7.2	Inducción de personal
Gestión de tecnología	9.1 y 9.1.a	Medición de indicadores de tecnología y seguimiento y medición de los controles del seguridad de la información
	A.9.4.3	Sistema de gestión de contraseñas
	A.11.2.8	Equipo de usuario desatendido
	A.9.3	Cumplimiento de políticas de contraseñas
	A.8.3.1	Política de USB-gestión de medios removibles

Fuente: Autor

6.14.5 Plan de cierre de no conformidades. Una vez presentado el informe de auditoría se elaboró en plan de cierre de no conformidades en el formato de Password. Ver Anexo A. Cuadro control de Acciones Correctivas, Preventivas y de Mejora, con codificación F-CAL-11

7 CRONOGRAMA

Para el desarrollo del trabajo de grado se ha definido un tiempo de 10 días. El cuadro 8 muestra la distribución del tiempo para cada una de las fases y actividades.

Cuadro 8. Cronograma

Fase	Actividad	Septiembre									
		D1	D2	D3	D4	D5	D6	D7	D8	D9	D10
Fase 1	Actividad 1										
	Actividad 2										
	Actividad 3										
	Actividad 4										
	Actividad 5										
	Actividad 6										
	Actividad 7										
	Actividad 8										
	Actividad 9										
	Actividad 10										
Fase 2	Actividad 11										
	Actividad 12										
	Actividad 13										
Fase 3	Actividad 14										
	Actividad 15										
	Actividad 16										
	Actividad 17										
	Actividad 18										
Fase 4	Actividad 19										
	Actividad 20										

Fuente: Autor

8 CONCLUSIONES

El resultado del presente trabajo considero la guía metodología planteada por la NTC-ISO/IEC 19011:2012, para la realización de auditorías, además de tener en cuenta el ciclo PHVA, que apoya el planteamiento de cada una de las actividades requeridas que facilita la gestión de todo el ciclo de auditoría en la organización.

El presente trabajo permitió el ajuste y actualización de los insumos (formatos) requeridos durante el desarrollo de la auditoria interna.

La empresa logró obtener un informe final de auditoria interna objetiva que permitió conocer el nivel madurez actual de du SGSI, así como las opciones de mejoras necesarias lograr el cumplimento del estándar acorde con la Norma NTC-ISO/IEC 27001:2013 y las obligaciones reglamentarias y contractuales.

A partir de los resultados se definió el plan de cierre de las No conformidades encontradas muy alineadas a la misión de Password. Adicionalmente, se plantearon las recomendaciones para el cierre de las observaciones encontradas.

Basado en el resultado de la auditoría, Password, debe enfocar sus esfuerzos en el cierre de las No conformidades, observaciones y en establecer la práctica de la mejora continua en cada uno de los requisitos exigidos.

La auditoría del SGSI de Password, presenta como resultado un total de 17 observaciones y 5 No conformidades menores.

9 RECOMENDACIONES

Fortalecer el ciclo de mejora continua de los requisitos del SGSI. Enfocándose en los dominios débiles identificados en la auditoria.

Fortalecer competencias técnicas, estratégicas y funcionales así como la cultura organizacional de los funcionarios de Password. A través de la mejora y actualización del plan de capacitación actual de la compañía definiendo más temas de Seguridad de la Información.

Ampliar el alcance actual del SGSI de tal manera que se cubra no solamente la ciudad de Cali, sino que se cubra la sede de Bogotá.

Realizar seguimiento al plan de cierre de las No conformidades y observaciones del informe de la auditoría interna.

Revisar, actualizar y hacer seguimiento y definir nuevos indicadores que permitan una medición eficaz del estado del SGSI.

Se sugiere que se realice una auditoría de seguimiento que permita validar el cierre de las No conformidades y observaciones, previo a la programación de la auditoría externa para re certificación del SGSI.

BIBLIOGRAFÍA

ECHENIQUE GARCIA, José Antonio. Auditoria Informática. 2 ed. México, México.: McGraw-Hill, 2001, 300 p. ISBN0-07-015352-3

DAVIS, Chris y Schiller, Mike y Wheeler Kevin. IT Auditing: Using Controls to Protect Information Assets. 2 ed. Estados Unidos.: McGraw-Hill, 2011, 513 p. ISBN 978-0-07-174239-9

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS. Directrices para la auditoria de sistemas de gestión. NTC-ISO/IEC 19011. Bogotá D.C.: ICONTEC, 2011. 59 p.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI). Visión general y Vocabulario. NTC-ISO/IEC 27000. Bogotá D.C.: ICONTEC, 2016. 38 p.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI). Requisitos. NTC-ISO/IEC 27001. Bogotá D.C.: ICONTEC, 2013. 25 p.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS. Tecnología de la información. Técnicas de seguridad. Código de Práctica para controles de seguridad de la información. GTC-ISO/IEC 27002 Bogotá D.C.: ICONTEC, 2015. 110 p.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS. Tecnología de la información. Técnicas de seguridad. Guía de implementación de un sistemas de gestión de seguridad de la información. GTC-ISO/IEC 27003. Bogotá D.C.: ICONTEC, 2012. 79 p.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS. Tecnología de la información. Técnicas de seguridad. Gestión del riesgo en seguridad de la información. NTC-ISO/IEC 27005. Bogotá D.C.: ICONTEC, 2009. 66 p.

ANEXO A (Informativo)

Cuadro control de Acciones Correctivas, Preventivas y de Mejora, con codificación F-CAL-11

Formaro-F-CAL-11 Cuadro Control de Acciones Correctivas, Preventivas y de Mejora											
Ítem	**Proceso**	**Descripción de la No conformidad real o potencial/ mejora**	**Descripción de la Acción**	**Tipo Acción**	**Origen de la NC**	**Fecha límite de implementación**	**Responsable**	**Fecha de Seguimiento**			**Observaciones generales**
				AC	**AIC**			**1**	**2**	**3**	
1	Gestión Tecnológica	Se evidencia Incumpliendo la política 6.5.4.3. Puertos UBS deshabilitados, del Manual de Políticas Seguridad de la Información. Se verifica el equipo de cómputo de la funcionaria Carolina Mejía, y se evidencian los puertos USB habilitados. Estos deberían estar bloqueados de acuerdo a la lista de usuarios con puertos autorizados.	*Bloquear los puertos USB del equipo de la funcionaria *Revisar todos los puertos de los equipos y validar si están habilitados los autorizados * Revisión de periódica de la política de bloqueo de USB	x	x	**dic-16**	Auxiliar de infraestructura, comunicaciones y soporte	oct-16	nov-16	dic-16	

Formaro-F-CAL-11 Cuadro Control de Acciones Correctivas, Preventivas y de Mejora											
Ítem	**Proceso**	**Descripción de la No conformidad real o potencial/ mejora**	**Descripción de la Acción**	**Tipo Acción**	**Origen de la NC**	**Fecha límite de implementación**	**Responsable**	**Fecha de Seguimiento**			**Observaciones generales**
				AC	**AIC**			**1**	**2**	**3**	
2	Gestión Tecnológica	Se evidencia incumplimiento de la política de Usuario Desatendido del Manual de Política. SI M-GES-01. El Equipo de la auxiliar administrativa Carolina Mejía, no estaba configurado el bloqueo automático. Adicionalmente, Se observó equipos de los ingenieros John Martínez y Cesar Trujillo, cuentan con configuraciones diferentes a las definidas en el Procedimiento de Control de Acceso P-TEC-01. Numeral 4, viñeta 7.	*Configurar el bloqueo automático de sesión del equipo de la funcionaria *Revisar los equipos de los funcionarios y asegurarse que todos están configurados para bloqueo automático de sesión cada 5 minutos * Revisión periódica de la política de usuario desatendido.	x	x	**nov-16**	Auxiliar de infraestructura, comunicaciones y soporte	nov-16			

Formaro-F-CAL-11 Cuadro Control de Acciones Correctivas, Preventivas y de Mejora											
Ítem	**Proceso**	**Descripción de la No conformidad real o potencial/ mejora**	**Descripción de la Acción**	**Tipo Acción**	**Origen de la NC**	**Fecha límite de implementación**	**Responsable**	**Fecha de Seguimiento**			**Observaciones generales**
				AC	**AIC**			**1**	**2**	**3**	
3	Gestión Tecnológica	No existen evidencias de la revisión a las estaciones de trabajo. Se evidencia el riesgo de acceso no autorizado a sistemas y aplicaciones	*Revisar las estaciones de trabajo y dejar evidencia documentada de la revisión * Definir un cronograma de revisión de las estaciones de trabajo	x	x	**nov-16**	Auxiliar de infraestructura, comunicaciones y soporte	nov-16			
4	Gestión Tecnológica	Al revisar los indicadores del proceso se evidencia que no se realizó medición del indicador de copias de respaldo y de mantenimiento en el segundo trimestre del 2016. Incumpliendo de este modo el numeral 9.1 de la norma ISO 27001:2013 y la frecuencia definida en el listado maestro de indicadores F-GES-02.	*Realizar la medición de los indicadores de copias de respaldo y mantenimiento. * Obtener evidencia de la revisión los indicadores que se realiza de la reunión mensual del Sistema de Gestión de Seguridad de la	x	**x**	**nov-16**	Auxiliar de infraestructura, comunicaciones y soporte	nov-16			

Formaro-F-CAL-11 Cuadro Control de Acciones Correctivas, Preventivas y de Mejora											
Ítem	**Proceso**	**Descripción de la No conformidad real o potencial/ mejora**	**Descripción de la Acción**	**Tipo Acción**	**Origen de la NC**	**Fecha límite de implementación**	**Responsable**	**Fecha de Seguimiento**			**Observaciones generales**
				AC	**AIC**			**1**	**2**	**3**	
			Información								
5	Gestión de Talento Humano	No existe evidencia de la inducción acerca de gestión de riesgos dada al ingeniero Ricardo Molina. Incumpliendo con el procedimiento P-HUM-01, específicamente en el numeral 6.4, en el cual se propone que el tiempo para la inducción es de 15 días hábiles.	*Realizar la inducción total del ingeniero Ricardo Molina *Establecer un responsable de las inducciones * Revisar periódicamente la completitud de la documentación de los funcionarios de Password	x	**x**	**nov-16**	Auxiliar Administrativa	dic-16			

PLANEACIÓN Y EJECUCIÓN DE LA AUDITORIA INTERNA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE PASSWORD CONSULTING SERVICES BAJO LA NORMA NTC-ISO/IEC27001:2013 Y PLAN DE ACCIÓN DE LAS NO CONFORMIDADES ENCONTRADAS

Andrea Viveros Quisoboni y Ricardo Herrera *Universidad Piloto de Colombia*

***Abstract*— This article makes an introduction to the world of auditing and management systems, specifically information security. Additionally, it explores the problem/opportunity that originated PLANNING AND IMPLEMENTATION OF THE INTERNAL AUDIT OF THE PASSWORD CONSULTING SERVICES' INFORMATION SECURITY MANAGEMENT SYSTEM UNDER NTC-ISO/IEC27001: 2013 STANDARD AND NON-ACTION PLAN CONFORMITIES FOUND - grade work describing the process used to perform a first-party audit in order to measure the effectiveness of the Password Consulting Services' Information Security Management System -, methodology to carry out an audit trail, the execution schedule of the audit, the development of the audit following the methodology proposed, and the conclusions and recommendations reached to the author of the degree work.**

***Palabras claves*— Auditoria, Hallazgos, Auditoria Interna, No Conformidad, Observación, Criterios, Procesos, Sistema de Gestión de Seguridad de la Información.**

I. INTRODUCCIÓN

Las auditorías internas también llamadas auditorías de primera parte, actualmente tienen gran relevancia en las empresas que cuentan con Sistemas de Gestión, debido a que una adecuada gestión de los procesos son un pilar para lograr los objetivos estratégicos y obtener cumplimiento de los aspectos legales y contractuales, además de un posicionamiento en el mercado. La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basados en la adopción de las mejores prácticas o en una o más metodologías o marcos tales como: ISO/IEC 27001:2013, ITIL, COBIT, es un mecanismo para apoyar tales objetivos.

En el presente trabajo de grado, se plantea la estrategia que permitirá la gestión de la auditoria interna del SGSI de Password Consultig Serivces, bajo la Norma NTC-ISO/IEC 27001:2013. Inicialmente se propone realizar la planeación y ejecución de la Auditoria Interna y posteriormente definir el Plan de Acción de las No Conformidades Encontradas. A continuación se especifica el orden de la auditoría:

- Contexto: Definición de auditoría interna, Auditoria de Proveedores, auditorias de tercera partes, SGSI
- Metodología: Descripción y argumentación.
- Desarrollo: Descripción de actividades
- Informe: Descripción de resultados
- Plan de Cierre de No Conformidades

II. CONTEXTO

A. *Definición Auditoria.*

De acuerdo a la ISO 19011:2012 (ISO 19011:2012) auditoria es un proceso sistemático, independiente y documentado para obtener evidencias de la auditoria y evaluarlas de manera objetiva con el fin de determinar el grado en que se cumple los criterios de la auditoría.

1) Auditoria Interna:

Según la ISO 19011:2012 (ISO 19011:2012) la auditoría interna, denominada en algunos casos como auditoría de primera parte, se realiza por, o en nombre de, la propia organización, para la revisión por la dirección y con otros fines internos (ej. para confirmar la efectividad del sistema de gestión o para obtener información para la mejora del sistema de gestión)

2) *Auditoria Externa*

Finalmente la auditoría externa incluye lo que se denomina auditoría de segunda y tercera parte. La auditoría de segunda parte se lleva a cabo por partes que tienen un interés en la organización, tal como los clientes, o por otras personas en su nombre. Las auditorías de tercera parte se llevan a cabo por organizaciones. Las auditorias independientes y externas, tales como aquellas que proporcionan el registro o la certificación de conformidad.

A continuación se listan los principios de la auditoria

- Integridad
- Presentación ecuánime
- Debido cuidado personal
- Confidencialidad
- Independencia
- Enfoque basado en la evidencia

B. *Sistema de Gestión de Seguridad de la Información*

Según ISO 27001 (ISO 27001:2013) el Sistema de Gestión de Seguridad de la Información es un conjunto de diseños de procesos, sistemas de información y controles que permitan preservar la confidencialidad, integridad y disponibilidad de la información, basado en través de un proceso de gestión del riesgo. A continuación se definen los principios de la Seguridad de la Información:

1) Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados
.

2) Integridad: Propiedad de la información relativa a su exactitud y completitud.

3) *Disponibilidad:* Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

III. PROBLEMA/OPORTUNIDAD

Las auditorias son procesos que constituyen un todo, están en el continuo acercamiento a encontrar errores y fallos del sistema y permiten determinar una serie de recomendaciones y conclusiones que constituyen un juicio profesional de manera imparcial y acertada. En cumplimiento del programa anual de auditorías del sistema integrado de gestión y del sistema de gestión de seguridad de la información, la compañía Password Consulting Services, debe atender esta necesidad, así como los requerimientos de certificación y legales en pro de mantener la alta calidad y la vigencia en los estándares de la compañía por ser una firma de gran reconocimiento y posicionamiento en el mercado actual.

El presente trabajo toma como base el programa de auditorías del 2016 de Password Consulting Services SAS y la falta de personal con las competencias e imparcial suficiente para su ejecución en la sede Cali, razón por la cual, no se ha cumplido con el seguimiento a los sistemas de gestión en el segundo periodo del 2016. La empresa decide realizar esta auditoría interna con personal de Bogotá con el fin de obtener un resultado más objetivo.

Para la compañía esta auditoria permite conocer el estado real de su SGSI, que a su vez permite tomar medidas correctivas que lleven al cumplimiento y calidad de los sistemas existentes, adicionalmente se pretende que la auditoría contemple la totalidad de los requisitos y controles de la norma y retroalimente al personal auditado enfatizando en el ciclo de mejora continua de los procesos.

IV. OBJETIVO PRINCIPAL DEL PROYECTO DE GRADO

Gestionar la auditoria interna del Sistema de Gestión de Seguridad de la Información bajo la Norma NTC-ISO/IEC 27001:2013. En Password Consulting Services.

V. OBJETIVOS ESPECIFICOS DEL PROYECTO DE GRADO

- Evaluar y estudiar el programa de auditoria anual de Password Consulting Services.
- Identificar, valorar y definir los criterios de la auditoria del Sistema de Gestión de Seguridad de la Información de Password Consulting Services.
- Elaborar, ajustar y aprobar las listas de verificación para los diferentes procesos de la empresa incluidos en el alcance del Sistema de Gestión de Seguridad de la Información.
- Elaborar, ajustar y obtener aprobación del programa de auditoria para el Sistema de Gestión de Seguridad de la Información de Password Consulting Services
- Ejecutar la auditoria en los diferentes procesos de acuerdo al programa de auditoria y con las listas de verificación aprobadas
- Elaborar y presentar el informe final de la auditoria registrando los hallazgos encontrados durante la actividad
- Elaborar y presentar un plan de cierre de no conformidades encontradas en la auditoria.

VI. PLANEACIÓN

La gestión del trabajo de grado se realizó de acuerdo a la metodología propuesta por la norma ISO 19011:2011 Directrices para la auditoría de Sistemas de Gestión.

La auditoría se realizó de acuerdo a la metodología del PHVA. A continuación, se describen las fases de la gestión de la auditoria interna descritas así:

- Planear la auditoría
- Ejecutar la auditoria
- Verificar la auditoría
- Informe de auditoría

De acuerdo a la metodología del Planear, Hacer, Verificar y Actuar. Tal y como se observa en la siguiente ilustración.

Ilustración 1. Metodología PHVA

Fuente propia

Las actividades de la auditoría se describen a continuación, de acuerdo a las fases propuestas en las metodologías planteadas

A. Fase 1: Planeación de la Auditoría

Actividad 1: Se elaboró el Plan de Trabajo, cronograma, riesgos, procedimientos y se gestionaron los recursos necesarios para la auditoría de primera parte al SGSI de PASSWORD.
Actividad 2: Se realizó una reunión con la funcionaria de PASSWORD, encargado del Sistema Integrado de Gestión y se definió el alcance de la auditoria.
Actividad 3: Se planeó la auditoría interna y se estudió la documentación e información de las áreas del alcance de la auditoría interna en PASSWORD.
Actividad 4: Se elaboró el plan de auditoría teniendo en cuenta los siguientes aspectos:

- Alcance de la auditoria (Proceso de gestión de proyectos, gestión estratégica, gestión de tecnología, gestión comercial, gestión de calidad y gestión de recursos humanos), Procesos del alcance de la certificación actual en ISO 27001
- Procedimientos del programa de auditoría;
- Criterios de auditoría;
- Métodos de auditoría;
- Selección de equipos auditores;
- Recursos necesarios, incluyendo viajes y hospedaje;
- Procesos para manejo de confidencialidad, seguridad de la información, salud y seguridad y otros temas similares.

Actividad 5: Seleccionar la metodología que se va a utilizar para la ejecución de las auditorías, (entrevista en sitio de trabajo).
Actividad 6: Seleccionar y asignar las responsabilidades de la auditoría individual al líder del equipo auditor.
Actividad 7: Elaboración de las listas de verificación para cada uno de los procesos que hacen parte del alcance definido previamente.
Actividad 8: Enviar las listas de verificación para la auditoría a PASSWORD, para la respectiva aprobación por parte de la gestora de calidad.
Actividad 9: Aprobación de las listas de verificación en el formato enviado previamente por PASSWORD, teniendo en cuenta los criterios definidos previamente.
Actividad 10: Programación de la visita para ejecución de la auditoría interna al SGSI de PASSWORD

B. Fase 2: Ejecución de la Auditoría

Actividad 11: Reunión de apertura de la auditoría interna con los líderes de las áreas que son parte del alcance de la auditoría PASSWORD.
Actividad 12: Diligenciar un acta de inicio de la auditoría donde se establezcan las condiciones, es decir, objetivo, alcance, equipo auditor, el programa de auditoria y se definan los cambios solicitados al programa de auditoria.
Actividad 13: Ejecución de los planes de auditoría a los procesos definidos en el alcance de acuerdo a las listas de verificación previamente definidas.

C. Fase 3: Elaboración de Informes de la Auditoría

Actividad 14: Recolección y Verificación de la información relevante a los objetivos, alcance y criterios de la auditoría y evidencias que conduzcan a encontrar hallazgos de auditoría.
Actividad 15: Evaluar los hallazgos contra los criterios de la auditoría a fin de determinar la veracidad de estos.
Actividad 16: Elaborar el informe preliminar de auditoria, especificando observaciones, no conformidades menores y mayores.
Actividad 17: Realizar reunión de cierre de auditoría con los líderes de los procesos, en esta reunión se debe presentar el informe preliminar de la auditoria.
Actividad 18: Elaborar acta de cierre de auditoria, dejar evidencia de las actividades de la reunión

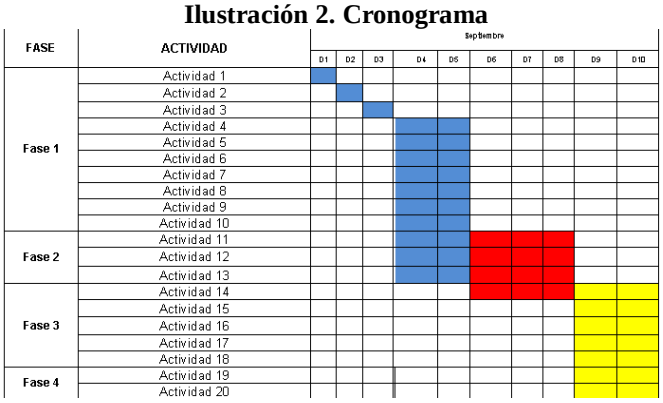
D. Fase 4: Monitoreo de la Auditoría

Actividad 20: Validar si se cumplieron los objetivos de la auditoria.
Actividad 21: Evaluar la auditoría, solicitar evaluación de auditores

VII. CRONOGRAMA

El tiempo total para gestión de la auditoria fue de 10 días distribuidos en planeación, ejecución y plan de cierre de no conformidades. A continuación se puede observar el cronograma de acuerdo a las actividades.

Ilustración 2. Cronograma



Fuente Propia

VIII. DESARROLLO

A continuación, de describen las actividades ejecutas antes, durante y después de la auditoría realizada al SGSI de Password Consulting Services

A. Fase 1: Planeación de la Auditoría

Se elaboró el Plan de Auditoria el cual incluye:

- Alcance de la auditoria
- Los criterios de auditoría
- El programa de auditoría
- El método de auditoría
- El equipo auditor
- Los recursos necesarios (incluyendo viajes y hospedaje)

Posteriormente se realizó una reunión con la líder del Sistema Integrado de Gestión de Password, con el fin de socializar el plan de auditoria.

1) Alcance de la auditoria

Se define como alcance de la auditoria interna del SGSI de Password, los siguientes procesos:

- Gestión de proyectos
- Gestión estratégica
- Gestión de tecnología
- Gestión comercial
- Gestión de calidad
- Gestión de recursos humanos

2) Criterios de auditoría

Una vez aprobado el alcance y obtenida la información se definieron los criterios por proceso así:

Gestión Integral: Se establece como criterios: la norma NTC-ISO/IEC 27001:2013, la caracterización del Proceso Vigente, los procedimientos de auditorías internas, de Acciones correctivas y preventivas, de Gestión de incidentes, Gestión de vulnerabilidades, Gestión de Activos, Clasificación y etiquetado, Gestión de cambios vigentes y la Metodológica gestión de riesgos

Gestión Comercial: Se establece como criterios: La Caracterización del proceso, Los documentos del proceso, las políticas de Seguridad de la Información y los requisitos de la Norma NTC-ISO/IEC 27001:2013

Gestión estratégica: Se establece como criterios; la Norma NTC-ISO/IEC 27001:2013, el Manual del SIG vigente, la matriz de comunicaciones y la caracterización del proceso

Gestión de Talento Humano: Se establece como criterios; la Norma NTC-ISO/IEC 27001:2013, el procedimiento de gestión de Talento humano, el procedimiento de contratistas, el Manual del SIG y la caracterización del proceso.

Gestión de Proyectos: Se establece como criterios; la Norma NTC-ISO 27001:2013, el Manual del SIG vigente, la caracterización del proceso de proyectos, el procedimiento análisis de seguridad, el procedimiento análisis forense, el procedimiento control de servicio no conforme y el procedimiento consultoría

Gestión Tecnológica: Se establece como criterios; La Norma ISO 27001:2013, la caracterización del proceso, los procedimientos aplicables, el Manual de Políticas de Seguridad, Procedimientos de tecnología y la declaración de aplicabilidad

3) Metodología de la auditoría

Se define como metodología para la ejecución de la auditoria, entrevistas en el puesto de trabajo de cada uno de los auditados

4) Equipo Auditor

El equipo auditor es conformado por la ingeniera Andrea Viveros Quisoboni, Coordinador de Proyectos Bogotá y por la Señora Diana Castillo, líder de Calidad de Password Consulting Services.

5) *Recursos*

Dado que el alcance de la auditoría interna, es en la ciudad de Cali Valle, se definen como recursos para la auditoría, los días laborales, los viáticos de los 3 días en la ciudad de Cali y los tiquetes de avión.

6) Acuerdo de Confidencialidad

Previo a la fecha de la auditoría se verifica la firma del acuerdo de confidencialidad contractual de la ingeniera Andrea Viveros y la Señora Diana castillo.

7) Plan de Auditoría

Posteriormente se procedió a elaborar y enviar el plan de auditoría a Password, sede Cali de acuerdo el alcance, los criterios, el equipo auditor y los auditados. Previa aprobación por parte de la Alta Dirección de la empresa se ejecutó la actividad que fue programada y ejecutada para el 20,21 y 22 de septiembre de 2016.

Se anexa el plan de auditoría

8) Listas de Verificación o Listas de Chequeo

Se elaboraron los planes de auditoría teniendo en cuenta los criterios anteriormente definidos y la siguiente matriz de requisitos aplicables de la Norma ISO/IEC 27001:2013

- Se anexan las listas de verificación

Ilustración 3. Matriz de Requisitos Aplicables

MATRIZ REQUISITOS APLICABLES (NORMA ISO 27001:2013 VS. PROCESOS)

No.	PROCESO	REQUISITOS	CONTROLES ANEXO A
1	Gestión comercial	6.1.2,6.1.3,8.2, 8.3,10.1	A.6.1.2,A.8.2.2,A.8.2.3,A.11.2.8,A.11.2.9,A .16.1.2, A.16.1.3,A.18.1.3, A.18.1.4, A.18.2.2
2	Gestión de proyectos	6.1.2,6.1.3,8.2, 8.3,10.1	A.6.1.2,A.6.1.5,A.8.2.2,A.8.2.3,A.11.2.8,A. 11.2.9,A.16.1.2, A.16.1.3A.18.1.3, A.18.1.4, A.18.2.2
3	Gestión Estratégica	6.1.2,6.1.3,7.1,8.1,8.2, 8.3,10.1	A.6.1.2,A.8.2.2 A.8.2.3,A.11.1,A.11.2.8,A.11.2.9, A.15,A.16.1.2, A.16.1.3,A.18.1.3, A.18.1.4, A.18.2.2
4	Gestión Talento Humano	5.3,6.1.2,6.1.3,7.2,7.3, 8.2, 8.3,10.1	A.6.1.1, A.7,A.8.1.4,A.8.2.2 A.8.2.3,A.11.2.8,A.11.2.9,A.16.1.2, A.16.1.3,A.18.1.3, A.18.1.4, A.18.2.2
5	Gestión de tecnología	6.1.2,6.1.3,8.2, 8.3,10.1	A.6.1.2, A.6.2,A.8.1.3,A.8.1.4,A.8.2.2,A.8.2.3,A.8.3. 1, A.8.3.2, A.8.3.3,A.9.1, A.9.2, A.9.3, A.9.4, A.10, A.11.2, A.12.1.1,A.12.1.3,A.12.1.4,A.12.2,A.12.3, A.12.4,A.12.5,A.12.6.2, A.13, A.14.1,A.14.2.4,A.16.1.2, A.17.2,A.18.1.3, A.18.1.4, A.18.1.5,A.18.2.2, A.18.2.3
6	Gestión integral	4.4,6.1,7.5,8.1,8.2,8.3, 9.1,9.2,10.1	A.6.1.2,A.6.1.3, A.6.1.4, A.8.1.1, A.8.1.2,A.8.1.3,A.8.2.1,A.8.2.2,A.8.2.3,A.1 1.2.8,A.11.2.9,A.12.1.2, A.12.6.1,A.12.7,A.13,A.16,A.17,A.18.1.3, A.18.1.4,A.18.2.1,A.18.2.2

Fecha de actualización: 18/09/2016

Fuente Propia

B. Fase 2 Ejecución de la Auditoria

Se ejecuta la auditoria de acuerdo al programa de auditoría previamente aprobado, se realiza la reunión de inicio, con una presentación en la cual se explican los objetivos, criterios, el equipo auditor, se pone a consideración el programa de auditoría en el caso de requerir un cambio en el itinerario.

Posteriormente se inicia con las entrevistas de acuerdo a la programación durante los dos días propuestos. Una vez ejecutadas las entrevistas en su totalidad se procede a entregar el primer informe la auditoría y se revisen las retroalimentaciones. La actividad queda consignada en el acta de cierre de auditoría.

- Se anexa acta de inicio, presentación y acta de cierre

C. Fase 3 Elaboración de Informes

Finalmente se realiza la recolección y verificación de la información que fue relevante para los objetivos, el alcance, los criterios de la auditoría y las evidencias que llevaron a definir hallazgos de auditoría, se procedió a evaluar los hallazgos contra los criterios de la auditoría, se determinó la veracidad de los hallazgos. Se presenta el informe preliminar de auditoria en la reunión de cierre de auditoría en esta reunión se logró especificar observaciones y No conformidades menores. Posteriormente, se envía el informe definitivo de la auditoria interna del SGSI de Password Consulting Services. A continuación, se describen los hallazgos de manera gerencial.

- Se anexa Informe Final AIC-Ciclo 1 -2016

IX. INFORME GERENCIAL

A. Nivel de Madurez del SGSI de Password

Producto de la auditoría realizada a Password Consulting Services, se determina que el nivel de madurez del SGSI, es del 89.5%. Los resultados detallados por clausulas y dominios del Anexo A. Se muestran a continuación en la tabla 4 y 5.

Tabla 1. Nivel de Madurez

Ítem	Cláusulas del SGSI	Cláusulas	Nivel de madurez Cláusulas
4..	Contexto de la Organización	100%	Optimizado
5..	Liderazgo	88%	Administrado
6..	Planificación	95%	Optimizado
7..	Soporte	88%	Administrado
8..	Operación	67%	Definido
9..	Evaluación del Desempeño	98%	Optimizado
10..	Mejora	91%	Optimizado
NIVEL DE MADUREZ		92%	Optimizado

Fuente Propia

Tabla 2. Nivel de Madurez

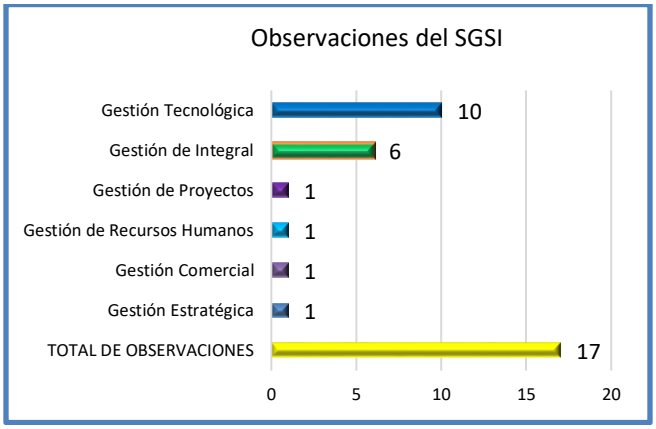
Ítem	Dominios	Controles	Nivel de madurez Dominios
A.5..	Política de Seguridad de la Información	100%	Optimizado
A.6..	Organización de la Seguridad de la Información	100%	Optimizado
A.7..	Seguridad en los Recursos Humanos	83%	Administrado
A.8..	Gestión de los activos	50%	Repetible
A.9..	Control de Acceso	96%	Optimizado
A.10..	Criptografía	50%	Repetible
A.11..	Seguridad Física y del Entorno	90%	Administrado
A.12..	Seguridad de las Operaciones	86%	Administrado
A.13..	Seguridad de las Comunicaciones	100%	Optimizado
A.14..	Adquisición, Desarrollo y Mantenimiento de Sistemas	100%	Optimizado
A.15..	Relaciones con los Proveedores	100%	Optimizado
A.16..	Gestión de incidentes de Seguridad de la Información	57%	Repetible
A.17..	Aspectos de seguridad de la información de la Gestión de Continuidad de Negocio	100%	Optimizado
A.18..	Cumplimiento	100%	Optimizado
NIVEL DE MADUREZ		**87%**	**Administrado**

Fuente Propia

B. Aspectos por mejorar/observaciones de la Auditoría

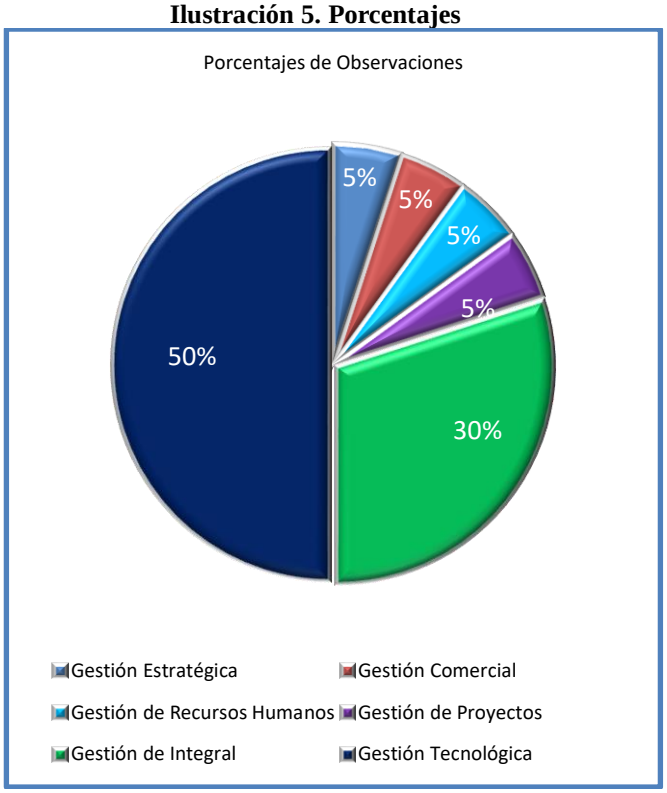
Como resultado de la auditoría se evidenciaron un total de 11, aspectos por mejorar y/o observaciones; El proceso de gestión tecnológica obtuvo un total de 10 observaciones correspondientes al 50%, el proceso de Gestión integral obtuvo un total de 6 observaciones correspondientes al 30%, el proceso gestión de recursos humanos, obtuvo una observación correspondiente al 5%, los procesos de gestión de proyectos, gestión comercial y gestión estratégica humanos obtuvieron observaciones compartidas correspondientes al 15% restante, como se observa en las Ilustración 4 y 5.

Ilustración 4. Observaciones



Fuente Propia

Ilustración 5. Porcentajes



Fuente Propia

C. No conformidades

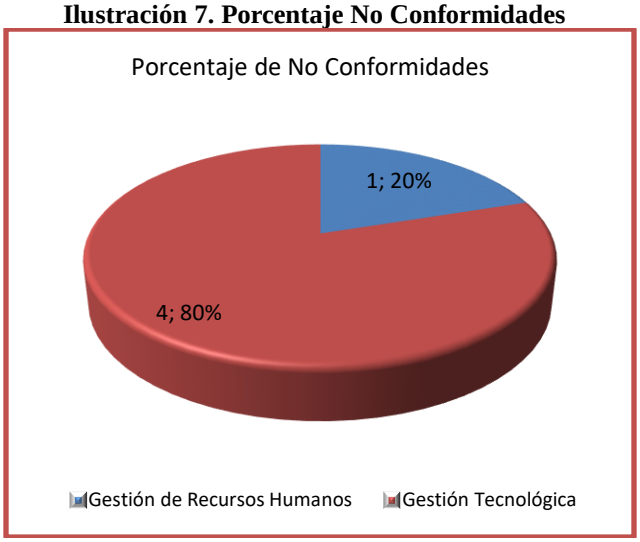
Como resultado de la auditoría se evidenciaron un total de 5 No conformidades menores; el proceso de gestión tecnológica obtuvo un total de 4. No conformidades Menores correspondientes al 80%, el proceso de recursos humanos obtuvo una No conformidad correspondiente al 20%, como se evidencia en las gráficas 6 y 7

Los procesos de gestión estratégica, gestión integral, gestión de proyectos y gestión comercial no obtuvieron No conformidades.

Ilustración 6. No Conformidades

Fuente Propia

Ilustración 7. Porcentaje No Conformidades



Fuente Propia

X. PLAN DE CIERRE DE NO CONFORMIDADES

Una vez presentado el informe de auditoría se elaboró en plan de cierre de no conformidades en los formatos de la empresa. Ver Anexo F-CAL-11 Cuadro Control AC-AP-AM-AIC-2-2016

XI. CONCLUSIONES

De acuerdo con el objetivo de la auditoria y los hallazgos encontrados podemos concluir:

- El resultado del presente trabajo considero la guía metodología planteada por la NTC-ISO/IEC 19011:2012, para la realización de auditorías, además de tener en cuenta el ciclo PHVA que apoya el planteamiento de cada una de las actividades requeridas que facilita la gestión de todo el ciclo de auditoría en la organización

- El presente trabajo permitió el ajuste y actualización de los insumos (formatos) requeridos durante el desarrollo de la auditoria interna.

- La empresa logró obtener un informe final de auditoria interna objetiva que permitió conocer el nivel madurez actual de du SGSI, así como las opciones de mejoras necesarias lograr el cumplimento del estándar acorde con la Norma NTC-ISO/IEC 27001:2013 y las obligaciones reglamentarias y contractuales

- A partir de los resultados se definió el plan de cierre de las No conformidades encontradas muy alineadas a la misión de Password Consulting Services. Adicionalmente, se plantearon las recomendaciones para el cierre de las observaciones encontradas.

- Basado en el resultado de la auditoría, Password Consulting Services debe enfocar sus esfuerzos en el cierre de las No conformidades, observaciones y en establecer la práctica de la mejora continua en cada uno de los requisitos exigidos.

- La auditoría del Sistema de Gestión de Seguridad de la Información de Password, presenta como resultado un total de 10 observaciones y 5 No conformidades menores.

XII. RECOMENDACIONES

- Fortalecer el ciclo de mejora continua de los requisitos del Sistema de Gestión de Seguridad de la Información. Enfocándose en los dominios débiles identificados en la auditoria

- Fortalecer tantas competencias técnicas, estratégicas y funcionales así como la cultura organizacional de los funcionarios de Password Consulting Services. A través de la mejora y actualización del Plan de Capacitación actual de la compañía definiendo más temas de Seguridad de la Información.

- Ampliar el alcance actual del Sistema de Gestión de Seguridad de la Información de tal manera que se cubra no solamente la ciudad de Cali, sino que se cubra la sede de Bogotá.

- Realizar seguimiento al plan de cierre de las No conformidades y observaciones del informe de la auditoría interna

- Revisar, actualizar y hacer seguimiento y definir nuevos indicadores que permitan una medición eficaz del estado del Sistema de Gestión de Seguridad de la Información.

- Se sugiere que se realice una auditoría de seguimiento que permita validar el cierre de las No conformidades y observaciones, previo a la programación de la auditoría externa para re certificación del SGSI

XIII. REFERENCIAS

• ECHENIQUE GARCIA, José Antonio. Auditoria Informática. 2 ed. México, México.: McGraw-Hill, 2001. 267p

• DAVIS, Chris y Schiller, Mike y Wheeler Kevin. IT Auditing: Using Controls to Protect Information Assets. 2 ed. Estados Unidos.: McGraw-Hill, 2011. Disponible en http://www.normas9000.com/que-es-iso-9000.html

• INSTITUTO COLOMBIANO DE NORMAS TECNICAS. Directrices para la auditoria de los sistemas de gestión de la calidad y/o ambiental. Bogotá D.C.: ICONTEC, 2012. 48 p. NTC-ISO 19011. Disponible en http://www.iso27000.es/iso27000.html

• INSTITUTO COLOMBIANO DE NORMAS TECNICAS. NTC-ISO/IEC 27001:2103 Tecnología de la Información. Técnicas de Seguridad Sistemas de Gestión de Seguridad de la Información. Requisitos.

• INSTITUTO COLOMBIANO DE NORMAS TECNICAS. NTC-ISO/IEC 27002:2015. Tecnología de la Información. Técnicas de Seguridad Código de Practica para Controles de Seguridad de la Información

XIV. AUTOR

Andrea Viveros Quisoboni es Ingeniera de Sistemas y Computación, con énfasis de seguridad de la información, egresada de la Universidad del Quindío, con experiencia y conocimientos en implementación de ISO 27001 y consultorías y auditorias en sistemas de información y bases de datos. Es certificada en auditor líder ISO 27001:2103. Experiencia y conocimientos sistemas operativos GNU/Linux y servidores. Participación y desarrollo de proyectos de ethical hacking para empresas del sector privado y gobierno.